**CSE 484 In-class Worksheet (Fall 2016)**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UWNetID: \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student ID #: \_\_\_\_\_\_\_\_\_\_

Partner names for this activity: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Q1:** Alice and Bob are talking using OTR. Bob receives a message MACed with their shared secret, so he’s sure that Alice sent it. Can he prove to Eve that Alice sent the message? Why or why not?

**Q2:** Perfect forward secrecy prevents eavesdropped messages from being decrypted if the clients are later hacked/controlled by the adversary. What are some ideas for how you could achieve this property?